(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－328901
（P2002－328901A）
(43)公開日　平成14年11月15日(2002.11.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８２
12/00	５３７	12/00	５３７Ａ	５Ｂ０８５

審査請求　未請求　請求項の数７　ＯＬ　（全 ７ 頁）

(21)出願番号　特願2001－133587(P2001－133587)

(22)出願日　平成13年４月27日(2001.4.27)

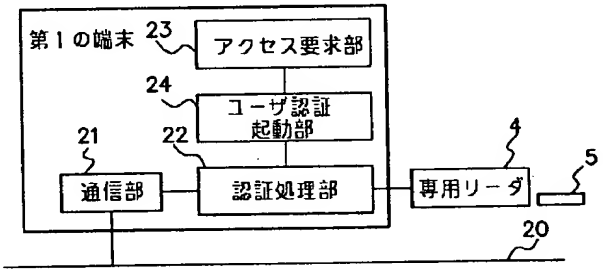
(71)出願人　399104844
住商情報システム株式会社
東京都中央区晴海１丁目８番12号
(72)発明者　加藤　道明
東京都墨田区両国２丁目10番14号　住商情報システム株式会社内
(74)代理人　100105784
弁理士　橘　和之

Ｆターム(参考)　5B082 EA11 HA08
5B085 AA08 AE02 AE03 AE12 AE25

(54)【発明の名称】　ユーザ認証システム、ユーザ認証の起動方法、ユーザ認証起動プログラム、記録媒体

(57)【要約】
【課題】　ユーザが意図的に認証機能を起動する必要をなくし、ユーザ認証を行うユーザの利便性を向上させることができるようにする。
【解決手段】　ネットワーク２０上の端末１にユーザ認証起動部２４を設け、アクセスする際にはユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたか否かを判断し、そのようなアクセス要求が行われたときにはユーザ認証の機能を自動的に起動するようにすることにより、ユーザが意図的にユーザ認証の機能を起動しなくても済むようにする。

第１の端末の機能構成例



【特許請求の範囲】

【請求項１】　アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断する判断手段と、

上記判断手段により上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手段とを備えたことを特徴とするユーザ認証システム。

【請求項２】　アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断ステップと、

上記アクセス判断ステップで上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動ステップとを有することを特徴とするユーザ認証の起動方法。

【請求項３】　アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断ステップと、

上記アクセス判断ステップで上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、既にユーザ認証が成立しているか否かを判断する認証成否判断ステップと、

上記認証成否判断ステップで上記ユーザ認証がまだ成立していないと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動ステップとを有することを特徴とするユーザ認証の起動方法。

【請求項４】　上記アクセス判断ステップは、何らかのアクセス要求が行われたか否かを判断する第１のステップと、

上記第１のステップで上記何らかのアクセス要求が行われたと判断したときに、そのアクセス要求が上記ユーザ認証が必要なネットワークもしくはシステムに対するアクセス要求か否かを判断する第２のステップとを有することを特徴とする請求項２または３に記載のユーザ認証の起動方法。

【請求項５】　アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断手順、および

上記アクセス判断手順で上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手順をコンピュータに実行させるためのユーザ認証起動プログラム。

【請求項６】　アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断手順、

上記アクセス判断手順で上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、既にユーザ認証が成立しているか否かを判断する認証成否判断手順、および上記認証成否判断手順で上記ユーザ認証がまだ成立していないと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手順をコンピュータに実行させるためのユーザ認証起動プログラム。

【請求項７】　請求項５または６の何れか１項に記載の各手順をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はユーザ認証システム、ユーザ認証の起動方法、ユーザ認証起動プログラム、記録媒体に関し、特に、ネットワークもしくは当該ネットワーク上のシステムに対してアクセスするのに必要なユーザ認証を受ける際のインタフェースの改良に関するものである。

【０００２】

【従来の技術】近年、インターネットやイントラネットなどのネットワークを利用した情報システムが広く用いられている。この情報システムにおいては、他人による不正侵入、情報漏洩、改ざん、情報システム自体の稼動妨害などをいかに防ぐかが重要な課題となっている。情報システムの安全を守るためのセキュリティシステムとしては幾つかの技術が存在するが、その中の１つに、ユーザ認証技術がある。

【０００３】ユーザ認証技術の代表的なものは、パスワードである。すなわち、個々のユーザが自分に割り当てられた固有のパスワードをキーボードなどから入力し、そのパスワードが個人認証システムにより照合されて正しいことが確かめられると、ネットワークや当該システム上のシステムへのアクセスができるようになるものである。

【０００４】ところが、近年においてはハッキング技術が向上し、パスワードを盗むことは簡単になってきている。そのため、パスワードによるユーザ認証では、他人による不正アクセスを完全に防止することは事実上不可能な状況になっている。そこで最近では、解読が困難なＩＣカードを利用したユーザ認証技術も用いられるようになってきている。

【０００５】さらに最近では、指紋や声、顔などを使って個人を識別する、いわゆるバイオメトリクス認証技術が注目され、開発されている。また、これとＩＣカードとを組み合わせた技術も開発されている。例えば、ユー

ザの指紋データをＩＣカードに格納しておき、ネットワーク等の利用時にそのＩＣカードを端末に挿入してユーザ本人の指紋データとを照合し、正しければネットワーク等へのアクセスを許可するようにしたものである。

【０００６】図４は、ユーザ認証技術を適用したネットワークシステムの構成例を示す図である。図４に示すシステムでは、第１、第２の端末１０１，１０２と、人事・給与サーバ１０６とがネットワーク１１０を介して接続されている。人事・給与サーバ１０６にはデータベース１０７が接続されており、人事・給与に関する各種データが格納されている。この各種データの中には、個人の学歴・懲罰・病歴・健康状態・給与などに関する個人情報も含まれている。

【０００７】第１、第２の端末１０１，１０２と人事・給与サーバ１０６との間には、個人認証装置１０５が設置されている。個人認証装置１０５は、データベース１０７上のデータが改ざんされたり、個人情報が盗まれたりするといった不都合を回避すべく、人事・給与サーバ１０６に対するアクセスを特定のユーザに対してのみ許可するために、ユーザ認証に関する処理を行うものである。

【０００８】第１の端末１０１には、ＩＣカード１０４の専用リーダ１０３が接続される。ＩＣカード１０４には、人事・給与サーバ１０６に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋・声・顔などのバイオメトリクス情報等）を格納しておく。

【０００９】従来、第１の端末１０１のユーザがネットワーク１１０を介して人事・給与サーバ１０６にアクセスする場合は、以下のような手順で実行していた。まず、第１の端末１０１の画面上に表示されたユーザ認証実行用のアイコンをユーザがクリックする。そして、画面に表示される指示に従ってＩＣカード１０４を専用リーダ１０３に挿入し、自分の認証情報を第１の端末１０１に読み取らせる。

【００１０】第１の端末１０１は、読み取った認証情報を個人認証装置１０５に送る。個人認証装置１０５は、第１の端末１０１から送られてきた認証情報を確認し、正しければ人事・給与サーバ１０６へのアクセスを許可する。人事・給与サーバ１０６へのアクセスが許可されると、そのことが第１の端末１０１に伝えられ、画面上にメッセージとして表示される。

【００１１】このメッセージを見たユーザは、第１の端末１０１の画面上に表示された人事・給与サーバ１０６の起動用のアイコンをクリックする。すると、人事・給与サーバ１０６が提供する初期画面が立ち上がり、以降当該人事・給与サーバ１０６が提供するサービスを受けることが可能となる。

【００１２】

【発明が解決しようとする課題】上述のユーザ認証技術を用いることにより、ネットワーク上に接続されたシステムの安全性を高めることが可能である。しかしながら、上記従来の技術では、ユーザが目的とするシステムにアクセスする前に、ユーザ認証実行用のアイコンをクリックして意図的にユーザ認証の機能を起動する必要がある。

【００１３】人間の心理として、あるシステムを利用しようとするときは、そのシステムを直接起動したいと考えるのが普通である。したがって、目的とするシステムを起動する前に、本来の利用目的とは全く関係のない余分な作業を行うために、わざわざユーザ認証の機能を起動しなくてはいけない従来の仕組みは、ユーザにとって非常に煩わしいものであった。また、何度もアイコンをクリックしてユーザ認証の機能や目的システムの機能をその都度起動しなくてはならないため、その操作が非常に面倒でもあった。

【００１４】本発明は、このような問題を解決するために成されたものであり、ユーザが意図的に認証機能を起動する必要をなくし、ユーザ認証を行うユーザの利便性を向上させることができるようにすることを目的とする。

【００１５】

【課題を解決するための手段】本発明のユーザ認証システムは、アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手段とを備えたことを特徴とする。

【００１６】また、本発明によるユーザ認証の起動方法は、アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断ステップと、上記アクセス判断ステップで上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動ステップとを有することを特徴とする。

【００１７】本発明の他の態様では、アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断ステップと、上記アクセス判断ステップで上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、既にユーザ認証が成立しているか否かを判断する認証成否判断ステップと、上記認証成否判断ステップで上記ユーザ認証がまだ成立していないと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動ステップとを有することを特徴とする。

【００１８】本発明のその他の態様では、上記アクセス判断ステップは、何らかのアクセス要求が行われたか否かを判断する第１のステップと、上記第１のステップで上記何らかのアクセス要求が行われたと判断したときに、そのアクセス要求が上記ユーザ認証が必要なネットワークもしくはシステムに対するアクセス要求か否かを判断する第２のステップとを有することを特徴とする。

【００１９】また、本発明のユーザ認証起動プログラムは、アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断手順、および上記アクセス判断手順で上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手順をコンピュータに実行させるためのものである。

【００２０】本発明の他の態様は、アクセスする際にはユーザ認証が必要なネットワークもしくは上記ネットワーク上のシステムに対してアクセス要求が行われたか否かを判断するアクセス判断手順、上記アクセス判断手順で上記ユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたと判断された場合に、既にユーザ認証が成立しているか否かを判断する認証成否判断手順、および上記認証成否判断手順で上記ユーザ認証がまだ成立していないと判断された場合に、上記ユーザ認証の機能を起動するユーザ認証起動手順をコンピュータに実行させるためのものである。

【００２１】また、本発明のコンピュータ読み取り可能な記録媒体は、請求項５または６の何れか１項に記載の各手順をコンピュータに実行させるためのプログラムを記録したことを特徴とする。

【００２２】

【発明の実施の形態】以下、本発明の一実施形態を図面に基づいて説明する。図１は、本実施形態によるユーザ認証システムの機能構成を示すブロック図であり、図２は、本実施形態のユーザ認証システムを適用したネットワークシステム全体の構成を示す図である。

【００２３】図２において、１，２，３はパーソナルコンピュータ等から成る端末、９はファイルサーバ、１０はメールサーバ、１１は人事・給与サーバ、１２は経理・財務サーバであり、これらがネットワーク２０を介して互いに通信可能なように接続されている。

【００２４】ファイルサーバ９は、ファイルの転送、削除、ディレクトリ操作などの処理を行う。メールサーバ１０は、端末１，２，３からの要求に基づいて電子メールを送信したり、届いた電子メールを保管して端末１，２，３からの照会があったときに引き渡したりする処理を行う。人事・給与サーバ１１は、企業内の人事・給与に関する様々な処理を行う。経理・財務サーバ１２は、企業内の経理・財務に関する様々な処理を行う。なお、これらの各種サーバ９～１２は公知のものを用いることが可能であるので、ここでは処理内容の詳細な説明は割愛する。

【００２５】８はルータであり、ネットワーク２０上の適当な位置に設置されている。あるコンピュータからネットワーク２０上に送信されたデータは、必ずルータ８を経由して目的とするコンピュータに届けられる。このルータ８は、ＩＰヘッダにある宛先ＩＰアドレスをもとに、ルータ８自身が持つ経路情報（ルーティングテーブル）を参照し、転送する次のノードを判断してデータを転送する。

【００２６】１３は個人認証装置であり、第１～第３の端末１～３と、人事・給与サーバ１１および経理・財務サーバ１２との間に設置されている。個人認証装置１３は、人事・給与サーバ１１、経理・財務サーバ１２に対するアクセスを特定のユーザに対してのみ許可するために、第１および第２の端末１，２から送られてくる認証情報に基づいてユーザ認証に関する処理を行う。

【００２７】第１の端末１には、ＩＣカード５の専用リーダ４が接続される。ＩＣカード５には、例えば人事・給与サーバ１１に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第１の端末１のユーザは、ファイルサーバ９とメールサーバ１０とに自由にアクセスすることができるとともに、ＩＣカード５を用いてユーザ認証を受けることで、人事・給与サーバ１１にもアクセスできるようになる。

【００２８】また、第２の端末２には、ＩＣカード７の専用リーダ６が接続される。ＩＣカード７には、例えば経理・財務サーバ１２に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第２の端末２のユーザは、ファイルサーバ９とメールサーバ１０とに自由にアクセスすることができるとともに、ＩＣカード７を用いてユーザ認証を受けることで、経理・財務サーバ１２にもアクセスできるようになる。

【００２９】第３の端末３は、ユーザ認証を受けるための機能を備えていない。すなわち、第３の端末３のユーザは、人事・給与サーバ１１および経理・財務サーバ１２に対するアクセス権を持っておらず、ファイルサーバ９とメールサーバ１０に対してのみアクセスすることが可能である。

【００３０】なお、ここでは第１および第２の端末１，２の外付けでＩＣカード５，７の専用リーダ４，６を設ける構成としたが、第１および第２の端末１，２自体がＩＣカード５，７の読み取り機能を備えていても良い。また、ここではユーザ認証を受けるためにＩＣカード５，７を用いているが、本発明はユーザ認証の方法は特に限定しない。例えば、パスワードなどの他のユーザ認証技術を用いても良い。

【００３１】また、ここでは、アクセスするのにユーザ認証を必要とするものを人事・給与サーバ１１および経理・財務サーバ１２としたが、これらのサーバに限定されるものではない。例えば、図示しない他のサーバもしくはファイルサーバ９やメールサーバ１０、または図示しないホストコンピュータなどについても、個人認証装置１３によるユーザ認証をアクセスの前提条件とするようにしても良い。

【００３２】図１に示すブロック図は、図２中に示した第１の端末１の機能構成例を示すものである。なお、第２の端末２も第１の端末１と同様に構成されるので、ここでは図示を省略する。図１において、２１は通信部であり、ネットワーク２０を介してデータの送受信に関する処理を行う。２２は認証処理部であり、個人認証装置１３と共動してユーザ認証に関する処理を行う。

【００３３】上記認証処理部２２は、専用リーダ４にて読み取ったＩＣカード５内の認証情報を取り込み、通信部２１を介して個人認証装置１３に送信する機能を有している。また、個人認証装置１３から通信部２１を介して送られてくる認証許可情報を取り込み、保持する機能も有している。認証処理部２２が認証許可情報を保持している間だけ、人事・給与サーバ１１にアクセスすることが可能である。

【００３４】２３はアクセス要求部であり、ユーザがファイルサーバ９、メールサーバ１０および人事・給与サーバ１１にアクセスすることを要求するための処理を行うものである。具体的には、アクセス要求部２３は、第１の端末１の画面上に表示されるＧＵＩ（Graphical User Interface）による起動用アイコンを含む。ユーザがマウスでこのアイコンをクリックすることにより、ファイルサーバ９、メールサーバ１０あるいは人事・給与サーバ１１に対するアクセスを要求する。

【００３５】なお、これらのサーバ９，１０，１１の起動方法は、アイコンを用いた起動方法に限られるものではない。例えば、メニューバーからポップアップあるいはプルダウン表示される起動用メニューを選択することによって、各サーバ９，１０，１１に対するアクセスを要求するようにしても良いことは言うまでもない。本発明では、各サーバ９，１０，１１の起動方法は特に限定しない趣旨である。

【００３６】２４はユーザ認証起動部であり、アクセス要求部２３により人事・給与サーバ１１に対するアクセス要求が行われたときに、認証処理部２２によりユーザ認証を行うための機能を自動的に起動する。これにより、専用リーダ４のカードスロットにＩＣカード５を挿入することをユーザに要求する。これに応じてユーザは、ＩＣカード４を専用リーダ５に挿入し、自分の認証情報を第１の端末１に読み取らせてユーザ認証を実行する。

【００３７】このユーザ認証起動部２４は、本発明の判断手段およびユーザ認証起動手段に相当するものである。実際には第１の端末１のＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成され、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって上述したユーザ認証起動部２４の機能構成が実現される。

【００３８】したがって、第１の端末１が上記ユーザ認証起動部２４の機能を果たすように動作させるプログラムを例えばＣＤ－ＲＯＭのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。上記プログラムを記録する記録媒体としては、ＣＤ－ＲＯＭ以外に、フロッピー（登録商標）ディスク、ハードディスク、磁気テープ、光ディスク、光磁気ディスク、ＤＶＤ、不揮発性メモリカード等を用いることができる。また、上記プログラムをネットワーク２０を介して他のコンピュータからダウンロードするようにしても良い。

【００３９】また、第１の端末１が供給されたプログラムを実行することによりユーザ認証起動部２４の機能が実現されるだけでなく、そのプログラムが第１の端末１において稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部が第１の端末１の機能拡張ボードや機能拡張ユニットにより行われて上述の機能が実現される場合も、かかるプログラムは本発明の実施形態に含まれる。

【００４０】図３は、ユーザ認証起動部２４の動作を示すフローチャートである。図３において、ユーザ認証起動部２４は、アクセス要求部２３によりアクセス要求が行われたかどうかを監視している（ステップＳ１）。何らかのアクセス要求が行われた場合は、それが人事・給与サーバ１１に対するアクセス要求かどうかを判定する（ステップＳ２）。

【００４１】ここでは、人事・給与サーバ１１のＩＰアドレスとアクセス要求が行われたＩＰアドレスとが一致するかどうかを見ることによって、アクセス要求が人事・給与サーバ１１に対するものであるかどうかを判定する。ユーザ認証を必要とする人事・給与サーバ１１のＩＰアドレスは、あらかじめ指定しておけば良い。

【００４２】人事・給与サーバ１１に対するアクセス要求でない場合、すなわち、ファイルサーバ９およびメールサーバ１０へのアクセス要求であった場合は、ユーザ認証を行うことなく自由にアクセスが可能なので、ユーザ認証に関しては何ら処理を行うことなくステップＳ１に戻る。この場合は、アクセス要求されたファイルサーバ９あるいはメールサーバ１０の機能が実行されることとなる（図示せず）。

【００４３】一方、人事・給与サーバ１１に対するアクセス要求であった場合、ユーザ認証が既に行われて成立済みかどうかを判定する（ステップＳ３）。ユーザ認証

が既に成立しているかどうかは、認証処理部２２により認証許可情報が保持されているかどうかを見ることによって判断することが可能である。

【００４４】なお、ユーザ認証の成否の判断方法は、この例に限定されるものではない。例えば、人事・給与サーバ１１に対するアクセス要求が行われたときに、通信部２１を介して個人認証装置１３にユーザ認証の成否を問い合わせるようにしても良い。この場合は、個人認証装置１３が認証許可情報を保持することになる。

【００４５】本実施形態では、第１の端末１の画面上に、従来と同様にユーザ認証実行用のアイコンも表示させ、このアイコンをクリックすることによってユーザ認証の機能を意図的に起動することも可能なようにしている。したがって、人事・給与サーバ１１に対してアクセス要求が行われたときには既に、ユーザ認証が成立済みの場合もある。ユーザ認証が既に成立している場合は、ステップＳ１に戻る。

【００４６】一方、ユーザ認証がまだ成立していない場合（ユーザ認証処理がまだ行われていない場合）は、認証処理部２２によりユーザ認証を行うための機能を自動的に起動する（ステップＳ４）。これに応じてユーザは、第１の端末１の画面上に表示される指示に従ってＩＣカード４を専用リーダ５に挿入し、自分の認証情報を第１の端末１に読み取らせてユーザ認証を実行する。

【００４７】なお、ここでは、第１の端末１において人事・給与サーバ１１に対するアクセス要求が行われたときにおけるユーザ認証起動部２４の動作を示したが、第２の端末２において経理・財務サーバ１２に対するアクセス要求が行われたときも、第２の端末２内のユーザ認証起動部２４によって同様の処理が行われる。

【００４８】以上詳しく説明したように、本実施形態においては、ユーザ認証を必要とする指定のサーバへのアクセスが発生したときに、ユーザ認証プログラムを自動的に起動するようにしているので、ユーザは意図的に認証機能を起動しなくても済む。

【００４９】これにより、ユーザは、今から何がやりたいかという自分の目的に沿って操作を行えば良くなり、わざわざ認証機能を起動するという煩わしさから開放される。また、目的のサーバにアクセスするためにアイコンを１回クリックすれば良く、ユーザ認証のためにも別にアイコンをクリックする必要がなくなる。よって、１回のクリック操作で目的サーバへのアクセスも認証機能の起動も行うことができ、ユーザの操作手続を簡便にすることができる。

【００５０】また、本実施形態では、ユーザ認証が必要な指定のサーバにアクセスしたときに、既にユーザ認証が済んでいる場合は、再度ユーザ認証機能を起動することがない。すなわち、本実施形態によれば、ユーザ認証機能の不必要な自動起動は行わないようにすることができる。

【００５１】なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００５２】

【発明の効果】本発明は上述したように、アクセスする際にはユーザ認証が必要なネットワークもしくはシステムに対してアクセス要求が行われたか否かを判断し、そのようなアクセス要求が行われたときにはユーザ認証の機能を起動するようにしたので、ユーザが意図的にユーザ認証の機能を起動しなくても済むようにすることができる。これにより、ユーザは、本来の利用目的を実行する前にわざわざ認証機能を起動するという煩わしさから開放され、また、１回の操作で目的のシステム等へのアクセスも認証機能の起動も行うことができ、ユーザの操作手続を簡便にすることができる。以上のことから、本発明によれば、ユーザ認証を行うユーザの利便性を向上させることができる。

【図面の簡単な説明】

【図１】本実施形態による第１の端末の機能構成例を示すブロック図である。

【図２】本実施形態によるユーザ認証システムを適用したネットワークシステム全体の構成を示す図である。

【図３】本実施形態による第１の端末に備えられるユーザ認証起動部の動作を示すフローチャートである。

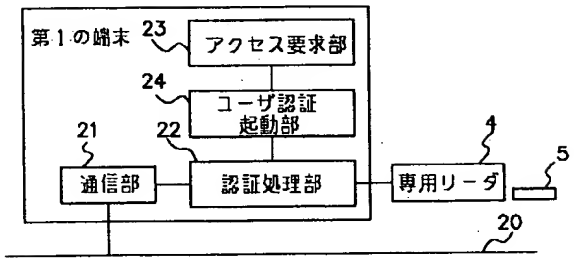
【図４】従来のネットワークシステム全体の構成を示す図である。

【符号の説明】

１，２，３　端末（パーソナルコンピュータ）
４，６　専用リーダ
５，７　ＩＣカード
８　ルータ
９　ファイルサーバ
１０　メールサーバ
１１　人事・給与サーバ
１２　経理・財務サーバ
１３　個人認証装置
２１　通信部
２２　認証処理部
２３　アクセス要求部
２４　ユーザ認証起動部

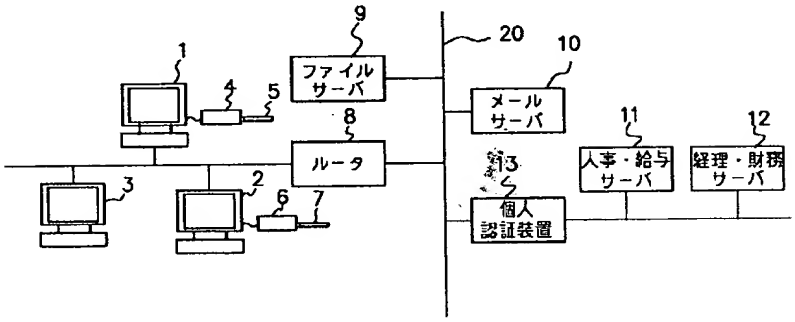
【図１】

第１の端末の機能構成例



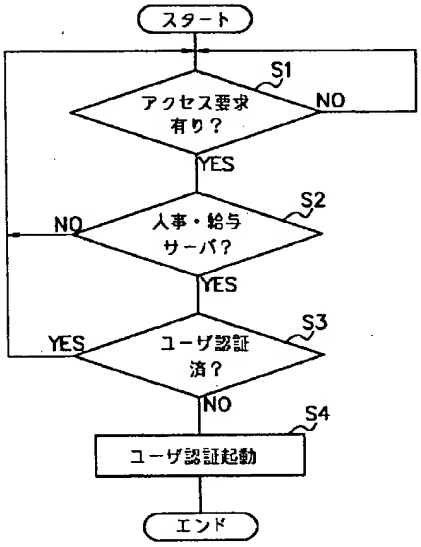
【図２】

ネットワークシステムの構成例



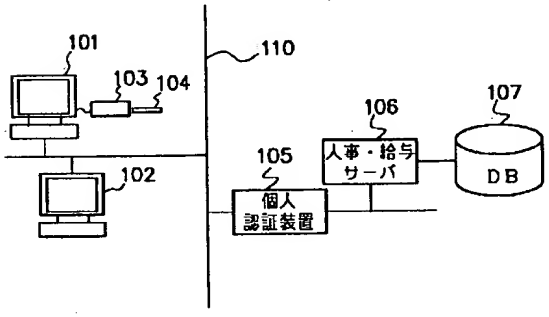
【図３】

ユーザ認証起動部の動作フロー



【図４】

従来のネットワークシステム



---

(54) USER AUTHENTICATION SYSTEM, USER AUTHENTICATION STARTING METHOD, USER AUTHENTICATION PROGRAM AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve convenience of a user for whom a user authentication is executed by eliminating a need for the user to start an authentication function intentionally.

SOLUTION: A user authentication starting part 24 is provided to a terminal 1 on a network 20, which, in accessing, judges whether a request for an access is made to a network or a system needing a user authentication. When the request for the access is made, the user authentication function is started automatically, thereby eliminating the user's need to start the authentication function intentionally.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-328901

(43)Date of publication of application : 15.11.2002

---

(51)Int.Cl. G06F 15/00

G06F 12/00

---

(21)Application number : 2001-133587 (71)Applicant : SUMISHO COMPUTER SYSTEMS CORP

(22)Date of filing : 27.04.2001 (72)Inventor : KATO MICHIAKI

LEGAL STATUS [Date of request for examination] 13.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The user authentication system characterized by having a decision means to judge whether the access request was performed to the system on the network which needs user authentication, or the above-mentioned network in case it accesses, and a user authentication starting means to start the function of the above-mentioned user authentication when it is judged that the access request was performed by the above-mentioned decision means to the network or system which needs the above-mentioned user authentication.

[Claim 2] The starting approach of the user authentication characterized by to have the access decision step which judges whether the access request was performed to the system on the network which needs user authentication in case it accesses, or the above-mentioned network, and the user-authentication starting step which starts the function of the above-mentioned user authentication when it is judged that the access request was performed to the network or the system which needs the above-mentioned user authentication at the above-mentioned access decision step.

[Claim 3] The access decision step which judges whether the access request was performed to the system on the network which needs user authentication in case it accesses, or the above-mentioned network, The authentication success-or-failure decision step which judges whether user authentication is

already materialized when it is judged that the access request was performed to the network or system which needs the above-mentioned user authentication at the above-mentioned access decision step, The starting approach of the user authentication characterized by having the user authentication starting step which starts the function of the above-mentioned user authentication when it is judged that the above-mentioned user authentication is not materialized yet at the above-mentioned authentication success-or-failure decision step.

[Claim 4] the 1st step, as for the above-mentioned access decision step, a certain access request judges it to be whether it was carried out or not, and the 1st step of the above -- the above -- the starting approach of user authentication according to claim 2 or 3 that the access request is characterized by having the 2nd step which judges whether it is an access request to the network or system which needs the above-mentioned user authentication when it judges that the access request of some kind was performed.

[Claim 5] The user authentication bootstrap for making a computer perform the user authentication activation procedure which starts the function of the above-mentioned user authentication, when accessing and it is judged that the access request was performed by the access decision procedure of judging whether the access request having been performed to the system on the network which needs user authentication, or the above-mentioned network, and

the above-mentioned access decision procedure, to the network or system which needs the above-mentioned user authentication.

[Claim 6] The access decision procedure of judging whether the access request having been performed to the system on the network which needs user authentication in case it accesses, or the above-mentioned network, When it is judged that the access request was performed by the above-mentioned access decision procedure to the network or system which needs the above-mentioned user authentication The authentication success-or-failure decision procedure of judging whether user authentication already being materialized, And the user authentication bootstrap for making a computer perform the user authentication activation procedure which starts the function of the above-mentioned user authentication, when it is judged that the above-mentioned user authentication is not materialized yet in the above-mentioned authentication success-or-failure decision procedure.

[Claim 7] The record medium which is characterized by recording the program for making a computer perform each procedure of a publication on any 1 term of claims 5 or 6 and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to amelioration of the interface at the time of receiving user authentication required accessing to the system on a network or the network concerned especially about a user authentication system, the starting approach of user authentication, a user authentication bootstrap, and a record medium.

[0002]

[Description of the Prior Art] In recent years, the information system using networks, such as the Internet and intranet, is used widely. In this information system, it has been an important technical problem how the unauthorized entry by others, an information leak, an alteration, operation active jamming of the information system itself, etc. are prevented. Although some techniques exist as a security system for keeping the insurance of an information system, a user authentication technique is in one of them.

[0003] The typical thing of a user authentication technique is a password. That is, each user enters from a keyboard etc. the password of a proper assigned to itself, and if the password is collated by the personal authentication system and

the right thing is confirmed, it comes to be able to perform access to the system on a network or the system concerned.

[0004] However, a hacking technique improves in recent years and it is becoming easy to steal a password. Therefore, in user authentication with a password, it is a situation impossible as a matter of fact to prevent unlawful access by others completely. So, recently, the user authentication technique with which decode used the difficult IC card is also used increasingly.

[0005] Furthermore, recently, the so-called biometric-person-authentication technique of identifying an individual using a fingerprint, voice, a face, etc. attracts attention, and is developed. Moreover, the technique which combined this and an IC card is also developed. for example, a user's fingerprint data -- an IC card -- storing -- network utilization time -- the IC card -- a terminal -- inserting -- a user -- his fingerprint data are collated, and if right, access to a network etc. will be permitted.

[0006] Drawing 4 is drawing showing the example of a configuration of the network system which applied the user authentication technique. In the system shown in drawing 4 , the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106 are connected through the network 110. The database 107 is connected to personnel affairs and the salary server 106, and the various data about personnel affairs and a salary are stored. In these various data, the

individual humanity news about individual school education, punishment, clinical recording, health condition, salary, etc. is also contained.

[0007] Personal authentication equipment 105 is installed between the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106. That it should avoid un-arranging [that the data on a database 107 are altered or individual humanity news is stolen], personal authentication equipment 105 performs processing about user authentication, in order to permit access to personnel affairs and the salary server 106 only to a specific user.

[0008] The exclusive reader 103 of IC card 104 is connected to the 1st terminal 101. The authentication information (biometrics information, such as a user's status information, or a fingerprint, voice, a face, etc.) about the user who has an access privilege to personnel affairs and the salary server 106 is stored in IC card 104.

[0009] When the user of the 1st terminal 101 accessed personnel affairs and the salary server 106 through a network 110 conventionally, it was performing in the following procedures. First, a user clicks on the icon for user authentication activation displayed on the screen of the 1st terminal 101. And IC card 104 is inserted in the exclusive reader 103 according to the directions displayed on a screen, and the 1st terminal 101 is made to read one's authentication information.

[0010] The 1st terminal 101 sends the read authentication information to personal authentication equipment 105. Personal authentication equipment 105 checks the authentication information sent from the 1st terminal 101, and if right, it will permit access to personnel affairs and the salary server 106. If access to personnel affairs and the salary server 106 is permitted, that will be told to the 1st terminal 101 and will be displayed as a message on a screen.

[0011] The user who looked at this message clicks on the icon for starting of the personnel affairs and the salary server 106 displayed on the screen of the 1st terminal 101. Then, the initial screen which personnel affairs and the salary server 106 offer starts, and it becomes possible to receive the service which personnel affairs and the salary server 106 concerned offer henceforth.

[0012]

[Problem(s) to be Solved by the Invention] By using an above-mentioned user authentication technique, it is possible to raise the safety of the system connected on the network. However, before a user accesses the target system, it is necessary to click on the icon for user authentication activation, and to start the function of user authentication intentionally in the above-mentioned Prior art.

[0013] As human being's psychology, when it is going to use a certain system, usually it is thought that he wants to start the system directly. Therefore, before starting the target system, in order to do the excessive activity which is

completely unrelated, the conventional structure which must start the function of user authentication specially was very troublesome [the original use purpose] for the user. Moreover, the actuation was also very troublesome, in order to have to click on an icon repeatedly and to have to start the function of user authentication, and the function of the purpose system each time.

[0014] This invention is accomplished in order to solve such a problem, it abolishes the need that a user starts an authentication function intentionally, and aims at enabling it to raise the convenience of the user who performs user authentication.

[0015]

[Means for Solving the Problem] The user authentication system of this invention is characterized by having a decision means to judge whether the access request was performed to the system on the network which needs user authentication, or the above-mentioned network in case it accesses, and a user authentication starting means to start the function of the above-mentioned user authentication when it is judged that the access request was performed by the above-mentioned decision means to the network or system which needs the above-mentioned user authentication.

[0016] Moreover, in case the starting approach of the user authentication by this invention accesses, it carries out having the access decision step which judges

whether the access request was performed to the system on the network which needs user authentication, or the above-mentioned network, and the user-authentication starting step which start the function of the above-mentioned user authentication when it is judged that the access request was performed to the network or the system which needs the above-mentioned user authentication at the above-mentioned access decision step as the description.

[0017] The access decision step which judges whether the access request was performed to the system on the network which needs user authentication in other modes of this invention in case it accesses, or the above-mentioned network, The authentication success-or-failure decision step which judges whether user authentication is already materialized when it is judged that the access request was performed to the network or system which needs the above-mentioned user authentication at the above-mentioned access decision step,. When it is judged that the above-mentioned user authentication is not materialized yet at the above-mentioned authentication success-or-failure decision step, it is characterized by having the user authentication starting step which starts the function of the above-mentioned user authentication.

[0018] the 1st step, as for the above-mentioned access decision step, a certain access request judges it to be whether it was carried out or not in the mode of others of this invention, and the 1st step of the above -- the above -- when it

judges that the access request of some kind was performed, the access request is characterized by having the 2nd step the above-mentioned user authentication judges it to be whether it is an access request to a required network or a required system.

[0019] Moreover, when the user-authentication bootstrap of this invention accesses and it is judged that the access request was performed by the access decision procedure judge whether the access request was performed to the system on the network which needs user authentication, or the above-mentioned network, and the above-mentioned access decision procedure, to the network or system which needs the above-mentioned user authentication, it is for making a computer perform the user-authentication activation procedure which starts the function of the above-mentioned user authentication.

[0020] The access decision procedure of judging whether the access request having been performed to the system on the network which needs user authentication in case other modes of this invention access, or the above-mentioned network, When it is judged that the access request was performed by the above-mentioned access decision procedure to the network or system which needs the above-mentioned user authentication When it is judged that the above-mentioned user authentication is not materialized yet in the authentication success-or-failure decision procedure of judging whether user

authentication already being materialized, and the above-mentioned authentication success-or-failure decision procedure, it is for making a computer perform the user authentication activation procedure which starts the function of the above-mentioned user authentication.

[0021] Moreover, the record medium which can computer read this invention is characterized by recording the program for making a computer perform each procedure of a publication on any 1 term of claims 5 or 6.

[0022]

[Embodiment of the Invention] Hereafter, 1 operation gestalt of this invention is explained based on a drawing. Drawing 1 is the block diagram showing the functional configuration of the user authentication system by this operation gestalt, and drawing 2 is drawing showing the configuration of the whole network system which applied the user authentication system of this operation gestalt.

[0023] In drawing 2 , personnel affairs and a salary server, and 12 are connected so that a file server and 10 may be accounting and a financial server a mail server and 11 and, as for the terminal with which 1, 2, and 3 consist of a personal computer etc., and 9, these can communicate mutually through a network 20.

[0024] A file server 9 processes transfer of a file, deletion, directory actuation, etc. A mail server 10 performs processing handed over when the electronic mail

was transmitted, or the delivered electronic mail is kept and there is enquiry from terminals 1, 2, and 3 based on the demand from terminals 1, 2, and 3. Personnel affairs and the salary server 11 perform various processings about the personnel affairs and the salary in a company. Accounting and the financial server 12 perform various processings about the accounting and financial affairs in a company. In addition, since these various servers 9-12 can use a well-known thing, detailed explanation of the contents of processing is omitted here.

[0025] 8 is a router and is installed in the suitable location on a network 20. The data transmitted on the network 20 from a certain computer are surely sent to the target computer via a router 8. This router 8 judges the following node to transmit based on the destination IP address in IP header with reference to the path information (routing table) which router 8 self has, and transmits data.

[0026] 13 is personal authentication equipment and is installed between the 1st - the 3rd terminal 1-3, and personnel affairs, the salary server 11 and accounting and a financial server 12. Personal authentication equipment 13 performs processing about user authentication based on the authentication information sent from the 1st and 2nd terminals 1 and 2, in order to permit access to personnel affairs and the salary server 11, and accounting and a financial server 12 only to a specific user.

[0027] The exclusive reader 4 of IC card 5 is connected to the 1st terminal 1. The

authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to personnel affairs and the salary server 11 is stored in IC card 5. The user of the 1st terminal 1 can also access personnel affairs and the salary server 11 by receiving user authentication using IC card 5 while being able to access a file server 9 and a mail server 10 freely.

[0028] Moreover, the exclusive reader 6 of IC card 7 is connected to the 2nd terminal 2. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to accounting and the financial server 12 is stored in IC card 7. The user of the 2nd terminal 2 can also access accounting and the financial server 12 by receiving user authentication using IC card 7 while being able to access a file server 9 and a mail server 10 freely.

[0029] The 3rd terminal 3 is not equipped with the function for receiving user authentication. That is, it does not have an access privilege to personnel affairs, the salary server 11, and accounting and a financial server 12, but the user of the 3rd terminal 3 can be accessed only to a file server 9 and a mail server 10.

[0030] In addition, although considered as the configuration which forms the exclusive readers 4 and 6 of IC cards 5 and 7 by external [of the 1st and 2nd terminals 1 and 2] here, the 1st and 2nd terminals 1 and 2 the very thing may be

equipped with the reading function of IC cards 5 and 7. Moreover, although IC cards 5 and 7 are used in order to receive user authentication here, this invention does not limit especially the approach of user authentication. For example, other user authentication techniques, such as a password, may be used.

[0031] Moreover, although what needs user authentication for accessing was made into personnel affairs, the salary server 11, and accounting and a financial server 12, it is not limited to these servers here. For example, it may be made to consider as the prerequisite of access to the user authentication by personal authentication equipment 13 also with other servers or file servers 9 which are not illustrated, a mail server 10, or the host computer which is not illustrated.

[0032] The block diagram shown in drawing 1 shows the example of a functional configuration of the 1st terminal 1 shown in drawing 2 . In addition, since it is constituted like [the 2nd terminal 2] the 1st terminal 1, illustration is omitted here. In drawing 1 , 21 is the communications department and performs processing about transmission and reception of data through a network 20. 22 is the authentication processing section, moves together with personal authentication equipment 13, and performs processing about user authentication.

[0033] The above-mentioned authentication processing section 22 incorporates the authentication information in IC card 5 read by the exclusive reader 4, and

has the function transmitted to personal authentication equipment 13 through the communications department 21. Moreover, the authentication authorization information sent through the communications department 21 from personal authentication equipment 13 is incorporated, and it also has the function to hold. Only while the authentication processing section 22 holds authentication authorization information, it is possible to access personnel affairs and the salary server 11.

[0034] 23 is the access request section and processing for a user to demand to access at a file server 9, a mail server 10, and personnel affairs and a salary server 11 is performed. Specifically, the access request section 23 contains the icon for starting by GUI (Graphical User Interface) displayed on the screen of the 1st terminal 1. When a user clicks on this icon with a mouse, access to a file server 9, a mail server 10, or personnel affairs and a salary server 11 is required.

[0035] In addition, the starting approach of these servers 9, 10, and 11 is not restricted to the starting approach which used the icon. For example, it cannot be overemphasized by choosing from a menu bar the menu for starting by which pop up or a pulldown indication is given that you may make it require access to each servers 9, 10, and 11. In this invention, especially the starting approach of each servers 9, 10, and 11 is the unlimited meaning.

[0036] 24 is the user authentication starting section, and when the access

request to personnel affairs and the salary server 11 is performed by the access request section 23, it starts automatically a function for the authentication processing section 22 to perform user authentication. This requires a user to insert IC card 5 in the card slot of the exclusive reader 4. According to this, a user inserts IC card 4 in the exclusive reader 5, makes the 1st terminal 1 read one's authentication information, and performs user authentication.

[0037] This user authentication starting section 24 is equivalent to the decision means and user authentication starting means of this invention. It consists of a CPU of the 1st terminal 1, MPU, RAM, ROM, etc. in fact, and the functional configuration of the user authentication starting section 24 mentioned above when the program memorized by RAM and ROM operated is realized.

[0038] Therefore, the program operated so that the 1st terminal 1 may achieve the function of the above-mentioned user authentication startup section 24 is recorded on a record medium like CD-ROM, and it can realize by making it read into a computer. As a record medium which records the above-mentioned program, a floppy (trademark) disk, a hard disk, a magnetic tape, an optical disk, a magneto-optic disk, DVD, a non-volatile memory card, etc. can be used in addition to CD-ROM. Moreover, you may make it download the above-mentioned program from other computers through a network 20.

[0039] moreover, the function of the user authentication starting section 24 is not

only realized by performing the program to which the 1st terminal 1 was supplied, but The case where an above-mentioned function is realized in collaboration with OS (operating system) or other application software etc. with which the program is working in the 1st terminal 1, Also when all or a part of supplied processing of a program is performed by the 1st functional add-in board and functional expansion unit of a terminal 1 and an above-mentioned function is realized, this program is included in the operation gestalt of this invention.

[0040] Drawing 3 is a flow chart which shows actuation of the user authentication starting section 24. In drawing 3 , the user authentication starting section 24 is supervising whether the access request was performed by the access request section 23 (step S1). When a certain access request is performed, it judges whether it is an access request to personnel affairs and the salary server 11 (step S2).

[0041] Here, an access request judges whether it is a thing to personnel affairs and the salary server 11 by obtaining whether the IP address of personnel affairs and the salary server 11 and the IP address to which the access request was carried out are in agreement. What is necessary is just to specify beforehand the IP address of personnel affairs and the salary server 11 which needs user authentication.

[0042] Since it can access freely, without performing user authentication when it

is not an access request to personnel affairs and the salary server 11 (i.e., when it is an access request to a file server 9 and a mail server 10), it returns to step S1, without processing in any way about user authentication. In this case, the function of the file server 9 or mail server 10 by which the access request was carried out will be performed (not shown).

[0043] On the other hand, when it is an access request to personnel affairs and the salary server 11, user authentication is already performed and judges whether it is finishing [formation] (step S3). Whether user authentication is already materialized can judge by seeing whether authentication authorization information is held by the authentication processing section 22.

[0044] In addition, the decision approach of the success or failure of user authentication is not limited to this example. For example, when the access request to personnel affairs and the salary server 11 is performed, you may make it ask personal authentication equipment 13 the success or failure of user authentication through the communications department 21. In this case, personal authentication equipment 13 will hold authentication authorization information.

[0045] With this operation gestalt, the icon for user authentication activation is also displayed as usual on the screen of the 1st terminal 1, by clicking on this icon, it is also possible to start the function of user authentication intentionally,

and it is made. Therefore, when an access request is performed to personnel affairs and the salary server 11, user authentication may already be formation ending. When user authentication is already materialized, it returns to step S1.

[0046] On the other hand, when user authentication is not materialized yet, a function for the authentication processing section 22 to perform user authentication is started automatically (step S4). (when user authentication processing is not performed yet) According to this, a user inserts IC card 4 in the exclusive reader 5 according to the directions displayed on the screen of the 1st terminal 1, makes the 1st terminal 1 read one's authentication information, and performs user authentication.

[0047] In addition, although here showed actuation of the user authentication starting section 24 when the access request to personnel affairs and the salary server 11 is performed in the 1st terminal 1, same processing is performed by the user authentication starting section 24 within the 2nd terminal 2 also when the access request to accounting and the financial server 12 is performed in the 2nd terminal 2.

[0048] Since he is trying to start a user authentication program automatically when access to the server of the assignment which needs user authentication occurs in this operation gestalt, as explained in detail above, it can be managed by him even if a user does not start an authentication function intentionally.

[0049] Thereby, what is necessary is just coming to operate it along with one's purpose, and it is wide opened from the troublesomeness of starting an authentication function specially. [whether a user wants what to do from now on] In order to access the target server, it becomes unnecessary moreover, to click on an icon independently also because of user authentication that what is necessary is just to click on an icon once. Therefore, access to the purpose server can also perform starting of an authentication function by one click actuation, and a user's actuation procedure can be made simple.

[0050] Moreover, when user authentication accesses the server of required assignment and user authentication can already be managed with this operation gestalt, a user authentication function is not started again. That is, it can avoid performing unnecessary auto-boot of a user authentication function according to this operation gestalt.

[0051] In addition, it does not pass over the operation gestalt explained above to what showed an example of the somatization which hits carrying out this invention, and the technical range of this invention must not be restrictively interpreted by this. That is, this invention can be carried out in various forms, without deviating from the pneuma or its main description.

[0052]

[Effect of the Invention] Even if a user does not start the function of user

authentication intentionally, it can make it possible to be managed, since this invention started the function of user authentication when having accessed, and it judged whether the access request was performed to the network or system which needs user authentication and such an access request was performed, as mentioned above. Thereby, access to the target system etc. can also perform starting of an authentication function by one actuation by being wide opened from the troublesomeness of starting an authentication function specially, before performing the original use purpose, and a user can make a user's actuation procedure simple. According to this invention, the convenience of the user who performs user authentication can be raised from the above thing.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the example of a functional configuration of the 1st terminal by this operation gestalt.

[Drawing 2] It is drawing showing the configuration of the whole network system which applied the user authentication system by this operation gestalt.

[Drawing 3] It is the flow chart which shows actuation of the user authentication

starting section with which the 1st terminal by this operation gestalt is equipped.

[Drawing 4] It is drawing showing the configuration of the conventional whole network system.

[Description of Notations]

1, 2, 3 Terminal (personal computer)

4 Six Exclusive reader

5 Seven IC card

8 Router

9 File Server

10 Mail Server

11 Personnel Affairs and Salary Server

12 Accounting and Financial Server

13 Personal Authentication Equipment

21 Communications Department

22 Authentication Processing Section

23 Access Request Section

24 User Authentication Starting Section